

FILED

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

2015 FEB 20 A 9:22

MICROSOFT CORPORATION, a
Washington corporation, and FS-ISAC, INC.,
a Delaware corporation,

Plaintiffs,

v.

JOHN DOES 1-3, CONTROLLING A
COMPUTER BOTNET THEREBY
INJURING PLAINTIFFS AND THEIR
CUSTOMERS AND MEMBERS,

Defendants.

CLERK US DISTRICT COURT
ALEXANDRIA, VIRGINIA

Civil Action No: 1:15 cv 240 LMB/IDD

**FILED UNDER SEAL PURSUANT TO
LOCAL CIVIL RULE 5**

**DECLARATION OF JASON LYONS IN SUPPORT OF PLAINTIFFS' APPLICATION
FOR AN EMERGENCY *EX PARTE* TEMPORARY RESTRAINING ORDER AND
ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION**

I, Jason Lyons, declare as follows:

1. I am a Senior Manager of Investigations in the Digital Crimes Unit of Microsoft Corporation's Legal and Corporate Affairs Group. I make this declaration in support of Plaintiffs' Application for An Emergency Temporary Restraining Order and Order To Show Cause Re Preliminary Injunction. I make this declaration of my own personal knowledge or on information and belief where noted. If called as a witness, I could and would testify competently to the truth of the matters set forth herein.

I. INTRODUCTION

2. In my role at Microsoft, I assess technological security threats to Microsoft and the impact of such threats on Microsoft's business and customers. Among my responsibilities are protecting Microsoft's online service assets from network-based attacks. I also participate in the investigation of botnets and participate in court-authorized countermeasures to disrupt them

and remediate their harmful effects. I have personally investigated and assisted in the court-authorized takedown of several botnets while at Microsoft, including the botnets known as ZeroAccess and Shylock. Before joining Microsoft, I worked for Xerox as the Manager of Xerox's Cyber Intelligence Response Team. I also worked for Affiliated Computer Services ("ACS") prior to Xerox's acquisition of ACS. While at ACS, I provided in-court testimony in connection with a temporary restraining order application concerning misappropriation of ACS's intellectual property. Prior to entering the private sector, from 1998 to 2005, I served as a Counterintelligence Special Agent in the United States Army. My duties as a Counterintelligence Special Agent included investigating and combating cyber-attacks against the United States. I obtained certifications in counterintelligence, digital forensics, computer crime investigations, and digital media collection from the United States Department of Defense. A current version of my curricula vitae is attached to this declaration as **Exhibit 1**.

3. I am a member of a team of investigators that has been investigating a botnet known as "Ramnit." The other investigators with whom I worked are co-declarants in this matter, and I refer the Court to their declarations for further information on particular aspects of Ramnit. I have reviewed the declarations of these individuals and concur in their conclusions. These investigators are the following:

- a. Karthik Selvaraj is a Senior Anti-Virus Researcher/Strategist in the Malware Protection Center of Microsoft. Mr. Selvaraj's declaration describes the general structure, operation, and propagation of Ramnit.
- b. Tim Liu is an Anti-Virus Researcher in the Malware Protection Center of Microsoft. Mr. Liu's declaration describes the internal functioning of Ramnit and how it harms both the user of the infected computer and the infected computer itself.
- c. Vikram Thakur is a Senior Manager with the Security Response Group at Symantec Corporation. Mr. Thakur's declaration describes the history of the

propagation of Ramnit as well as technical details of the manner in which Ramnit commits fraud against the computer user and the computer itself.

- d. Eric Guerrino is an Executive Vice President of FS-ISAC, Inc., the Financial Services Information Sharing & Analysis Center. Mr. Guerrino's declaration describes the impact of Ramnit and other similar financial-fraud botnets on the banking industry.

4. As part of our investigation, I and the other investigators purposely infected several investigator-controlled computers with Ramnit malware. This placed the computers under the control of the cybercriminals operating the botnet. We then monitored and analyzed the activities of the infected computers. Among other things, we observed the infected computers connect to and receive instructions from the Ramnit botnet's command and control servers. We carefully analyzed the changes Ramnit makes to Microsoft's operating system and application software during the infection process, and we reverse-engineered the Ramnit malware to determine how it operates. I personally participated in these investigative techniques. Further, I reviewed literature published by other well-regarded computer security investigators concerning Ramnit, and their findings have confirmed my own conclusions regarding the Ramnit botnet. Through these and related investigative steps, I have developed detailed information about the size, scope, and illegal activities of the Ramnit botnet.

5. In the remainder of this Declaration, I will explain
 - a. Ramnit's self-defense mechanisms that make countermeasures difficult; and
 - b. the proposed plan to disrupt Ramnit and significantly curtail the criminal activities Defendants perpetrate through Ramnit.

II. THE RAMNIT BOTNET'S COMMAND AND CONTROL INFRASTRUCTURE IS DESIGNED TO EVADE AND WITHSTAND TECHNICAL COUNTER-MEASURES

6. Ramnit is designed to be resistant to technical countermeasures. Therefore, part of my investigation involved understanding Ramnit's defensive features so as to better devise a plan to dismantle its harmful infrastructure.

A. Ramnit Has A Resilient Command And Control Infrastructure

7. A first set of defensive mechanisms makes the command and control structure of Ramnit resilient against counter-measures. Upon infecting a user's computer, each bot, or infected computer, generates a list of 300 domain names using a domain generation algorithm ("DGA"). The Ramnit DGA uses an algorithm to create a set of randomized domains. Promptly after generating the list of random domains, the infected computer begins to try to connect over the Internet with the domains. It continuously cycles through that list attempting to establish a connection. It does this until one of the domains answers back, confirming to the infected computer that it has established a connection with the Ramnit command and control infrastructure. Defendants can cause the infected computers to generate a new list of domains by updating the "seed" information used by the domain generation algorithm. There are several consequences of this that need to be addressed in any plan to disable Ramnit.

8. First, if Microsoft takes possession of only the currently active command and control domains, the Ramnit bots may resume attempting to contact the other domains in the list of 300 domains. To regain control of the bots, Defendants at that point need only register one of the 300 domains, associate it with an IP address on the Internet, and establish another command and control server at that address. Currently Defendants' command and control IP addresses resolve to servers across multiple countries in Europe. Therefore, it is necessary to take possession of all 300 domains, not just the domains that are currently being used.¹

¹ The currently active domains are associated with certain IP addresses. Some of the bots will continue to connect to those IP address even if Microsoft takes possession of the domain names because computers often store the IP addresses of frequently contacted domains. This civil action focuses on U.S.-based infrastructure, i.e., the Ramnit domains. Plaintiffs have relayed all underlying technical analysis of IP addresses, associated servers, and

9. Second, the Defendants could potentially update the “seed” used by the infected computers in the domain name generation algorithm and cause them to generate a new list of domain names.

10. If Defendants are able to shift the infected computers to a new command and control infrastructure before Ramnit is completely disabled, it would be futile to take possession of the set of domain names uncovered through our investigation, as the bots would be communicating with a completely new set of domains.

11. Further, based on my experience observing the operation of numerous botnets, prior legal actions involving botnets, and my observations of the specific architecture of the Ramnit botnet, I believe Defendants would take swift preemptive action to defend the botnet if they were to learn of Microsoft’s impending action against it. I am informed and believe there have been prior instances where security researchers or the government attempted to curb injury caused by botnets, but allowed the botnet operators to receive notice. In these cases, the botnet operators quickly moved the botnet infrastructure to new, unidentified locations on the Internet and took other countermeasures causing the botnet to continue its operations and destroying or concealing evidence of the botnet’s operations. Therefore, taking possession of the current command and control infrastructure must be done without giving prior notice to the Defendants.

12. In sum, a piecemeal or prematurely disclosed approach to disconnecting the Ramnit botnet’s command and control infrastructure will fail. Unless all traffic to any of the command and control domains is simultaneously redirected to secure computers, there is a chance that Defendants will be able to shift the command and control infrastructure to new domains. Further, unless all traffic to the command and control domains is simultaneously redirected to secure computers, Defendants may be able to access the infected computers, thus destroying evidence of their misconduct, their identities, and evidence of the infected computers

Defendants activities to law enforcement agencies throughout Europe. Plaintiffs understand that these agencies are monitoring this action and will take steps to disable Ramnit IP addresses abroad.

that connect to the command and control infrastructure. This would prevent mitigation and cleaning of those victims computers in the future.

B. Computers Infected With Ramnit Are Difficult To Clean

13. A second set of defensive mechanisms employed by the Ramnit botnet makes it difficult to clean infected computers and restore them to normal operation.

14. First, Ramnit encrypts communications between infected computers and the command and control infrastructure. This includes both configuration files and the stolen information uploaded from the infected computer. Over time, and in reaction to advances made by researchers attempting to defend against Ramnit and other similar botnets that employ encryption, Ramnit has deployed increasingly sophisticated encryption technology. Ramnit currently uses an RC4, asymmetric encryption technique to generate an RSA 1024 key. This makes it virtually impossible for security researchers to issue a command to each infected computer that would cause the bot on that computer to cease its operation, restore the computer to its pre-infection configuration, or uninstall itself.

15. Second, Ramnit disables anti-virus services on infected computers. The Ramnit malware contains a list of security related applications; this list is dynamic and has changed over time. When an infected computer attempts to run an executable file associated with a security application, the Ramnit malware kills the process, preventing the application from running. Ramnit specifically targets Microsoft anti-virus products.

C. Defendants Can “Kill” Infected Machines With One Command, Thereby Destroying Valuable Evidence And Cause Extreme Harm

16. Additionally the Defendants are capable of sending each infected computer encrypted “kill” command from the authoritative command and control infrastructure. Upon receiving that command, the Ramnit bot on the computer will delete certain critical information from the Windows registry that the Windows operating system needs to start, and will then turn the computer off, effectively making it impossible to restart the computer without repairing the operating system. Once the Ramnit kill command executes, Windows cannot boot on the

infected computer, and a user attempting to turn on the infected machine will simply see a blank blue screen on their monitor. This not only causes profound harm to the user of the computer, it also results in obfuscation of evidence of the Defendants' wrongdoing. Again, this makes it paramount that Microsoft be able to disable the command and control structure of Ramnit before Defendants learn of the action. As discussed above, Plaintiffs expect that law enforcement agencies in Europe will act promptly to mitigate the risk that Defendants will issue "kill" commands from servers in Europe.²

III. DISRUPTING RAMNIT

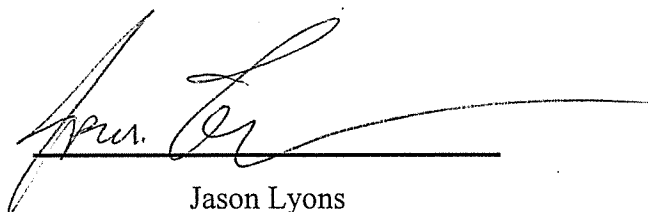
17. The most vulnerable point in Ramnit's architecture is the set of Internet domains and IP addresses of the command and control servers that Microsoft and its industry partners have identified through investigation of Ramnit. The Ramnit domains are listed in **Appendix A** to the Complaint in this matter. These are the domains from which those infected computers get their instructions on how to engage in the illegal activity. Granting Microsoft possession of the domains in Appendix A will enable Microsoft to channel all communications to those domains to secure servers, and thereby cut off the only means that Defendants have to communicate with the infected computers. In other words, any time an infected computer attempts to contact a command and control server through one of the domains, it will instead be connected to a Microsoft-controlled, secure server. As discussed above, seizing Ramnit IP addresses is also part of the Ramnit disruption strategy; as these IP addresses are located outside of this Court's jurisdiction, IP addresses will be dealt with via separate, coordinated action abroad.

18. I believe that the only way to suspend the injury caused to Microsoft, its consumers and the public, is to take the steps described in the [Proposed] *Ex Parte* Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("Proposed TRO"). This relief will significantly hinder the Ramnit botnet's monetization and capability and operational

² Even in the highly unlikely event that Defendants are able to issue kill commands that reach infected computers, it is possible to recover user files using commonly available software.

control. The domain registries and Internet service providers that provide services to the owners of the infected computers can notify them that they are infected and assist them in restoring their computers to normal operation.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge. Executed this 19th day of February, 2015, in Washington, D.C.



A handwritten signature in black ink, appearing to read "Jason Lyons", is written over a solid horizontal line. The signature is stylized and cursive.

Jason Lyons

Jason B. Lyons

17 Terra Evergreen Drive, Shady Shores, TX 76208,
940.497.5774, jasonblyons@gmail.com

SUMMARY

Jason Lyons is an experienced investigator specializing in computer investigations. Trained and experienced in hacker methodology/techniques, computer forensics, incident response, electronic discovery, litigation support and network intrusion investigations.

SECURITY CLEARANCE

- Top Secret/SCI-Expired.

CERTIFICATIONS

- Encase Certified Examiner (EnCE) - Guidance Software
- Sans Certified Incident Handler (GCIH)-SANS
- Counterintelligence Special Agent - Department of the Army
- Certified Basic Digital Media Collector - Department of Defense
- Certified Basic Computer Crime Investigator – Department of Defense
- Certified Basic Digital Forensic Examiner – Department of Defense
- State of Texas licensed Private Investigator

TECHNICAL SKILLS

- Network Intrusion Investigations
- Incident Response
- Investigative Network Monitoring
- Investigation Management/Liaison
- Computer Media Evidence Collection
- Computer Forensics
- EnCase Certified Examiner
- PDA and Cell Phone Seizure and Forensics
- Expert Witness Experience
- Technical/Investigative Report Writing

PROFESSIONAL EXPERIENCE

2012-Present Xerox Information Security Office
Cyber Intelligence Response Team (CIRT)
Manager of the CIRT

- Manager of the Cyber Intelligence Response Team (CIRT) for a fortune 500 company. Responsible for investigating, reporting, and responding to information security incidents worldwide.
- Manages an incident team who utilizes various forensic techniques to investigate information security incidents to include computer forensics, log analysis, network forensics, Intrusion Detection System (IDS) alerts, and malware analysis.
- Developed threat and risk matrices based on incidents types and report findings to upper management.
- Developed processes and procedures based on incident alerting sources, including escalated IDS alerts, MacAfee EPO, Email Spam filters, and Data Loss Prevention (DLP) alerts.
- Works with multiple vendors to develop proactive Proofs of Concepts (POC) to increase the company's security posture.

2005 – 2011

***Affiliated Computer Services, inc (ACS)/Xerox
Digital Forensic, eDiscovery Group
Manager of the Digital Forensics Group (DFG)***

- Manager of a fortune 500 company's digital forensic laboratory/group. Responsible for managing, coordinating, investigating, and reporting on legal, corporate security, human resources, and ethics investigations involving digital media.
- Developed policy and procedures for digital evidence acquisition, storage, examination, processing and production.
- Developed and maintained technical investigative support for ACS inside and outside legal counsel on eDiscovery matters. Experienced in developing and executing large eDiscovery collection plans, preserving data in a forensically sound manner, culling of relevant data, presenting data for review, hosting data for review, and producing relevant data for final production.
- Implemented Access Data's Enterprise and eDiscovery solution.

2003 – 2005

***Department of the Army, 902nd Military Intelligence (MI),
Cyber Counterintelligence Activity (CCA)
Assistant Operations Officer/Counterintelligence Special Agent***

- Assisted in managing of all CCA branch operations to include all cyber investigations, special intelligence collection missions, cyber investigator training, and quality assurance of all investigative products.
- Supervised 35 special agents and computer forensic technicians.
- Prepared detailed investigative briefings which include results of investigations and forensic analysis for executive level officers.
- Conducted national level liaisons with federal intelligence and law enforcement agencies on many national security investigations.
- Conducted network intrusion investigations, computer media forensics examinations, counterintelligence/counterterrorism special operations, and network forensic analysis.

2000 – 2003

***Department of the Army, 902nd MI, CCA
Counterintelligence Special Agent / Computer Investigator***

- Assistant Supervisory Special Agent (ASSA) of an eight man computer Incident Response Team (IRT) specializing in cyber investigations.
- Accountable for managing, editing and reviewing associated technical and investigative reports pertaining to the IRT's investigations.
- Provided and maintained incident response, computer forensics, evidence handling, and computer media search and seizure training for the members of the IRT.
- While assigned to the IRT, served as lead agent on numerous network intrusion and computer forensic Counterintelligence investigations.

1998-1999

***Department of the Army, 501st MI Brigade, South Korea
Counterintelligence Special Agent / Liaison Officer***

- Served as liaison officer for a Counterintelligence Resident Office in South Korea.
- Maintained regional-level liaison with foreign government officials to collect strategic information for intelligence reporting.
- Established business partnerships and furthered cooperation between the United States and South Korean investigative/intelligence agencies to accomplish bilateral goals.

EDUCATION

- Graduate from Excelsior College in October 2002, with a Bachelor of Science in Liberal Arts.
- Thirteen hours completed for Masters Degree in Information Technology with University of Maryland University College (UMUC).

TRAINING

- Counterintelligence Agent Course-Department of the Army-1998.
- Counterintelligence Fundamentals Warfare (CIFIW)-Department of the Army-2000.
- Introduction to Computer Search and Seizure-Defense Computer Investigation Training Program (DCITP), Linthicum, MD-2000.
- Introduction to Networks and Computer Hardware (INCH)-DCITP, Linthicum, MD-2000.
- Network Intrusion Analysis Course (NIAC)-DCITP, Linthicum, MD-2001.
- Computer Investigations for Special Agents (CICSA)-Department of the Army-2001.
- Basic Evidence Recovery Techniques (BERT)-DCITP, Linthicum, MD- 2002.
- Basic Forensic Examiner Course (BFE)-DCITP-Linthicum, MD-2002.
- Forensics in a Solaris Environment (FISE)-DCITP-Linthicum, MD-2002.
- SANS-Tracking Hackers/Honey pots-SANS Institute, Dupont Circle, DC-2003.
- Encase Intermediate Analysis and Reporting-Guidance Software, Sterling VA-2004.
- PDA and Cell Phone Seizure and Analysis-Paraben Software, Orlando FL-2005
- Network Monitoring Course (NMC)-DCITP- Linthicum, MD-2005
- Encase Advanced Internet Examinations-Guidance Software, Los Angeles CA-2006
- (FTK) Windows Forensics-AccessData, Dallas TX-2006
- (DNA) Applied Decryption-AccessData, Nashville TN, 2007
- Network Intrusion Course-Guidance Software, Houston, TX, 2010
- SANS-Hacker Techniques, Exploits, and Incident Handling, San Francisco, CA, 2011